ST-09-0002 WORKING DRAFT
OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

24 March 2009

(U) TABLE OF CONTENTS

WORKING DRAFT

I. (U) INTRODUCTION

Background

(U//FOUO) On 4 October 2001, President George W. Bush issued a memorandum entitled "AUTHORIZATION FOR SPECIFIED ELECTRONIC SURVEILLANCE ACTIVITIES DURING A LIMITED PERIOD TO DETECT AND PREVENT ACTS OF TERRORISM WITHIN THE UNITED STATES." The memorandum was based on the President's determination that after the 11 September 2001 terrorist attacks in the United States, an extraordinary emergency existed for national defense purposes.

(TS//SI//OR/NF) The 4 October 2001 Presidential authorization delegated authority to the Secretary of Defense, who further delegated it to the Director of National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) to conduct specified electronic surveillance on targets related to Afghanistan and international terrorism for 30 days. Because the surveillance included wire and cable communications carried into or out of the United States, it would otherwise have required FISC authority.

(TS//SI//OR/NF) The Authorization specified that NSA could acquire the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata[1] for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority. [2]

(U) This Report

(U//FOUO) This report provides the classified results of the NSA Office of the Inspector General (OIG) review of the President's Surveillance Program (PSP) as mandated in the FISA Amendments Act (FAA) of 2008. It includes the facts necessary to describe from NSA's perspective:

[1] (U)Metadata is data that describes content, events, or networks associated with SIGINT targets.

[2] (U)The Authority changed over time. See Appendix B for details.

ST-09-0002
WORKING DRAFT

- [X] establishment of the PSP (Section One)
- [X] implementation and product of the PSP (Section Two)
- [X] access to legal reviews of the PSP and access to information about the PSP (Section Three)
- [X] interaction with the Foreign Intelligence Surveillance Court (FISC) and transition to court orders related to the PSP (Section Four)
- [X] oversight of PSP activities at NSA (Section Five)

(U) President's Surveillance Program Terminology

(U//FOUO) For purposes of this report, the PSP, or "the Program," refers to NSA activities conducted under the authority of the 4 October 2001 memorandum and subsequent renewals, hereafter known as "the Authorization." As mandated by the FAA, this review includes activities authorized by the President between 11 September 2001 and 17 January 2007 and those activities continued under FISC authority. This includes the program described by the President in a 17 December 2005 radio address as the Terrorist Surveillance Program, which was content collected under the Authorization.

WORKING DRAFT

II. REVIEW CATEGORIES

(U) ONE: ESTABLISHMENT OF THE AUTHORITY

(U//FOUO) Immediately after the attacks of 11 September 2001, NSA considered how to work within existing SIGINT authorities to counter the terrorist threat within the United States and adjusted SIGINT processes accordingly. Shortly thereafter, in response to a White House request, the Director of NSA identified SIGINT collection gaps. The Counsel to the Vice President used this information to draft the Presidential authorization that established the PSP.

(U) Actions Taken After 9/11

(TS//SI//NF) On 14 September 2001, three days after terrorist attacks in the United States, General Hayden approved the targeting of terrorist-associated foreign telephone numbers on communication links between the United States and foreign countries where terrorists were known to be operating. Only specified, pre-approved numbers were allowed to be tasked for collection against U.S.-originating links. He authorized this collection at Special Collection Service and Foreign Satellite sites with access to links between the United States and countries of interest, including Afghanistan. According to the Deputy General Counsel, General Hayden determined by 26 September that any Afghan telephone number in contact with a U.S. telephone number on or after 26 September was presumed to be of foreign intelligence value and could be disseminated to the FBI.

(TS//SI//NF) NSA OGC said General Hayden's action was a lawful exercise of his power under Executive Order (E.O.) 12333, *United States Intelligence Activities*, as amended. The targeting of communication links with one end in the United States was a more aggressive use of E.O. 12333 authority than that exercised by former Directors. General Hayden was operating in a unique environment in which it was a widely held belief that additional terrorist attacks on U.S. soil were imminent. General Hayden said this was a "tactical decision."

(U//FOUO) On 2 October 2001, General Hayden briefed the House Permanent Select Committee on Intelligence (HPSCI) on this decision and later informed members of the Senate Select Committee on Intelligence (SSCI) by telephone. He had also informed DCI George Tenet.

(TS) At the same time NSA was assessing collection gaps and increasing efforts against terrorist targets immediately after the 11 September attacks, it was responding to Department of Defense (DoD), Director of Central Intelligence Community Management Staff questions about its ability to counter the new threat.

(U) Need to Expand NSA Authority

(U//FOUO) General Hayden said that soon after he told Mr. Tenet about NSA actions to counter the threat, Mr. Tenet shared the information with the "Oval Office." Mr. Tenet relayed that the Vice President wanted to know if NSA could be doing more. General Hayden replied that nothing else could be done within existing NSA authorities. In a follow-up telephone conversation, Mr. Tenet asked General Hayden what could be done if he had additional authorities. General Hayden said that these discussions were not documented.

(U//FOUO) NSA Identifies SIGINT Collection Gaps

(TS//SI//NF) To respond to the Vice President, General Hayden met with NSA personnel who were already working to identify and fill SIGINT collection gaps in light of the recent terrorist attacks. General Hayden stated that he met with personnel to identify which additional authorities would be operationally useful and technically feasible. In particular, discussions focused on how NSA might bridge the "international gap." An NSA Technical Director described that gap in these terms:

> *"Here is NSA standing at the U.S. border looking outward for foreign threats. There is the FBI looking within the United States for domestic threats. But no one was looking at the foreign threats coming into the United States. That was a huge gap that NSA wanted to cover."*

(TS//SI//NF) **Possible Solutions.** Among other things, NSA considered how to tweak transit collection—the collection of communications transiting through but not originating or terminating in the United States. NSA personnel also resurfaced a concept proposed in 1999 to address the

WORKING DRAFT

Millennium Threat. NSA proposed that it would perform contact chaining on metadata it had collected. Analysts would chain through masked U.S. telephone numbers to discover foreign connections to those numbers, without specifying, even for analysts, the U.S. number involved. In December 1999, the Department of Justice (DoJ), Office of Intelligence Policy Review (OIPR) told NSA that the proposal fell within one of the FISA definitions of electronic surveillance and, therefore, was not permissible when applied to metadata associated with presumed U.S. persons (i.e., U.S. telephone numbers not approved for targeting by the FISC).

(TS//SI//NF) **Collection gaps not adequately filled by FISA authorized intercept.** NSA determined that FISA authorization did not allow sufficient flexibility to counter the new terrorist threat. First, it believed that because of technological advances, the jurisdiction of the FISC went beyond the original intent of the statute. For example, most communications signals no longer flowed through radio ~~signals~~ signals or via phone systems as they did in 1978 when the FISA was written. By 2001, Internet communications were used worldwide, undersea cables carried huge volumes of communications, and a large amount of the world's communications passed through the United States. Because of language used in the Act in 1978, NSA was required to obtain court orders to target email accounts used by non-U.S. persons outside the United States if it intended to intercept the communications at a webmail service within the United States. Large numbers of terrorists were using such accounts in 2001.

(TS//SI//NF) Second, NSA believed that the FISA process was unable to accommodate the number of terrorist targets or the speed with which they changed their communications. From the time NSA sent FISA requests to the DoJ, OIPR until the time data arrived at NSA, the average wait was between four and six weeks. Terrorists could have changed their telephone numbers or internet addresses before NSA received FISC approval to target them. NSA believed the large number of terrorist targets and their frequently changing communications would have overwhelmed the existing FISA process.

(TS//SI//NF) Emergency FISA provision not an option. NSA determined that even using emergency FISA court orders would not provide the speed and flexibility needed to counter the terrorist threat. First, although the emergency authorization provision permitted 72 hours of surveillance without obtaining a court order, it did not—as many believed—allow the Government to undertake surveillance immediately. Rather, the Attorney General had to ensure that emergency surveillance would ultimately be acceptable to the FISC. He had to be certain the court

would grant a warrant before initiating emergency surveillance. Additionally, before NSA surveillance requests were submitted to the Attorney General, they had to be reviewed by NSA intelligence officers, NSA attorneys, and Department of Justice attorneys. Each reviewer had to be satisfied that standards had been met before the request proceeded to the next review group, and each request was certified by a senior official in the DoD, usually the Secretary or Deputy Secretary. From the time NSA sent a request to Justice's OIPR until the time data arrived at NSA, the average wait was between a day and a half. In the existing threat environment with U.S. interests at risk, NSA deemed the wait too long.

(U//FOUO) Early Efforts to Amend FISA

(TS//SI//NF) Given the limitations of FISA, there were early efforts to amend the statute. For example, shortly after 11 September, the HPSCI asked NSA for technical assistance in drafting a proposal to amend Section III of FISA that would give the President the authority to conduct electronic surveillances without a court order for the purpose of obtaining foreign intelligence information. On 20 September 2001, the NSA General Counsel wrote to Judge Alberto Gonzales, Counsel to the President, asking whether the proposal had merit. We found no record of a response.

(U//FOUO) We could not determine why early efforts to amend FISA were abandoned. Anecdotal evidence suggests that government officials feared the public debate surrounding any changes to FISA would compromise intelligence sources and methods.

(U) NSA identifies SIGINT collection gaps to Vice President's Office.

(TS//SI//NF) Because early discussions about expanding NSA's authority were not documented, we do not have records of specific topics discussed or people who attended General Hayden's meetings with White House representatives. General Hayden stated that after consulting with NSA personnel, he described to the White House how NSA collection of communications on a wire inside the United States was constrained by the FISA statute. Specifically, NSA could not collect from a wire in the United

WORKING DRAFT

States, without a court order, either content or metadata from communications links with either one or both ends in the United States. Furthermore, General Hayden pointed out that communications metadata did not have the same level of constitutional protection as content and that access to metadata of communications with one end in the United States would significantly enhance NSA's analytic capabilities. General Hayden suggested that the ability to collect communications with one end in the United States without a court order would increase NSA's speed and agility. General Hayden stated that after two additional meetings with the Vice President, the Vice President asked him to work with his Counsel, David Addington.

(U) Presidential Authorization Drafted and Signed

(TS//SI//OR/NF) According to General Hayden, the Vice President's Counsel, David Addington, drafted the first Authorization. General Hayden described himself as the "subject matter expert" but stated that no other NSA personnel participated in the drafting process, including the General Counsel. He also said that Department of Justice (DOJ) representatives were not involved in any of the discussions that he attended and he did not otherwise inform them.

(TS//SI//NF) General Hayden said he was "surprised with a small 's' " when the Authorization was signed on 4 October 2001, and that it only changed the location from which NSA could collect communications. Rules for minimizing U.S. person information still had to be followed.

(U//FOUO) SIGINT Activity Authorized by the President

(TS//SI//OR/NF) On 4 October 2001, the President delegated authority through the Secretary of Defense to the Director of NSA to conduct specified electronic surveillance on targets related to Afghanistan and international terrorism for 30 days. Because the surveillance included wire and cable communications carried into or out of the United States, it would otherwise have required FISC authority.

(TS//SI//STLW//NF) The Authorization allowed NSA to conduct four types of collection activity:

- Telephony content
- Internet content

ST-09-0002
WORKING DRAFT

- [X] Telephony metadata

- [X] Internet metadata

(TS//SI//NF) NSA could collect the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority.

(U//FOUO) Subsequent Changes to the Authorization

(TS//SI//NF) After the first Presidential authorization, the specific terms, wording, or interpretation of the renewals periodically changed. (See Appendix B for a completed listing of changes.)

(TS//SI//NF) **Domestic Collection.** The wording of the first authorization could have been interpreted to allow domestic content collection where both communicants were located in the U.S. or were U.S. persons. General Hayden recalled that when the Counsel to the Vice President pointed this out, General Hayden told him that NSA would not collect domestic communications because 1) NSA was a foreign intelligence agency, 2) NSA infrastructure did not support domestic collection, and 3) his personal standard was so high that there would be no problem getting a FISC order for domestic collection.

(TS//SI//NF) **Afghanistan.** In January 2002, after the Taliban was forced out of power, Afghanistan was no longer specifically identified in the Authorization.

(TS//SI//NF) **Iraqi Intelligence Service.** For a limited period of time surrounding the 2003 invasion of Iraq, the President authorized the use of PSP authority against the Iraqi Intelligence Service. On 28 March 2003, the DCI determined that, based on then current intelligence, the Iraqi Intelligence service was engaged in terrorist activities and presented a threat to U.S. interests in the United States and abroad. Through the Deputy DCI, Mr. Tenet received the President's concurrence that PSP authorities could be used against the Iraqi Intelligence Service. NSA ceased using the Authority for this purpose in March 2004.

WORKING DRAFT

(U) TWO: IMPLEMENTATION OF THE AUTHORITY AND RESULTING SIGINT PRODUCT

(TS//SI//NF) General Hayden said that although he felt comfortable exercising the Presidential authorization and believed it to be legal, he recognized that it was politically sensitive and controversial and would be subjected to scrutiny at some point in time. He and NSA leadership strove to ensure that NSA personnel executed the terms of the Authorization with care and diligence and that they not go beyond that which was authorized. PSP-related operations began on 6 October. Early on, personnel worked under the assumption that the Authorization was temporary and that operations would stop in the near future. After it became evident that the Authority would be continuously renewed, management focused on designing processes and procedures for Program activity.

(U//FOUO) Stand Up of Operations

(TS//SI//NF) On 4 October 2001, after receiving the Authorization, General Hayden informed the SIGINT Director and other key personnel of NSA's new authorities and asked the NSA General Counsel if the Authorization was legal. The General Counsel said that the next day, 5 October, he told General Hayden that he believed it was legal (see Appendix D).

(TS//SI//OC/NF) Under General Hayden's direction, immediate steps were taken to implement the temporary authority.

- A 24-hour watch operation, the Metadata Analysis Center (MAC), was created in the Signals Intelligence Directorate (SID).
- The first Program Manager was identified and informed of his new responsibilities.
- A cadre of experienced operational personnel was chosen to implement the Program.
- Office space was identified to accommodate newly assigned personnel.

- (U) A new security compartment with the temporary cover term STARBURST was established.[3]

- (U) Fifty computer servers to store and process data acquired under the new authority were ordered.[4]

- (U) Initial funding of $25 million for PSP operations was obtained from the DCI.

(TS//SI//NF) On Saturday and Sunday, 6 and 7 October, small groups of operational personnel were called at home and asked to report to work for special PSP clearance briefings.

(TS//SI//OR/NF) On Monday, 8 October 2001, Columbus Day, General Hayden briefed the analysts, programmers, and mathematicians that had been selected to implement the Authorization. At that briefing, General Hayden said he did not share the specific content of the Authorization with attendees but relayed key information such as:

- (U) The Authorization came from the President.

- (U) The Authorization was temporary.

- (U) The Authorization was intended to be an early warning system of impending terrorist attacks in the United States.

- (U) The NSA General Counsel had reviewed the Authorization and concluded that it was legal.

- (U) NSA would do exactly what the Authorization stated and "not one electron or photon more."

- (U) The Authorization should be kept secret and it required strict compartmentation. Attendees had to sign a non-disclosure agreement.

(TS//SI//NF) General Hayden stated that after he briefed the attendees, he turned the briefing over to the General Counsel to discuss the terms of the Authorization.

---

[3](TS//SI//NF) A permanent cover term, STELLARWIND, was assigned to Program information on 31 October 2001.

[4](TS//SI//NF) Because of the heightened terrorist threat, at NSA's request, a vendor diverted a shipment of servers intended for other recipients to NSA, where they arrived under police escort on 13 October 2001.

(U) Early Operations

(TS//SI//NF) Within one week, approximately 90 NSA employees were cleared for access to the PSP. On 11 October 2001, the Associate General Counsel for Operations and the NSA Deputy General Counsel were cleared for the Program and agreed with the NSA General Counsel's determination that the Authorization was legal. NSA OGC did not formally document its opinions or legal rationale (see Appendix D).

(TS//SI-STLW//NF) The MAC was created to analyze metadata obtained under PSP authorization. By 7 October 2001, it was a 24-hour 7-day a week watch center with 20 analysts, reporters, and software developers working in three shifts. Many MAC employees were former Russian traffic analysts with manual call chaining analysis experience. Initially, the MAC reported directly to General Hayden and the Deputy Director. The MAC Chief briefed the Director every week, and the Deputy Director visited MAC spaces for a briefing each evening.

(TS//SI//NF) While the MAC was setting up to analyze PSP metadata, the Counterterrorism (CT) Product Line was realigning to conduct PSP content tasking and analysis. The MAC and the CT Product Line worked closely together to coordinate efforts and share information. The CT Product Line was growing rapidly as handpicked employees were moved to support the new mission.

(TS//SI//NF) Within 30 days, the PSP was fully operational. While awaiting delivery of requested computer servers, the FBI and CIA gave NSA lead telephone numbers, and the MAC was able to immediately chain within the United States with SIGINT collected overseas. Private sector partners began to send telephony and Internet content to NSA in October 2001. They began to send telephony and Internet metadata to NSA as early as November 2001.

(U//FOUO) On-Going Operations

(TS//SI//NF) After operations began and it became evident that the Authorization was likely to be renewed indefinitely, NSA management became increasingly focused on designing processes and procedures to implement the Program effectively and to ensure compliance with the Authorization.

(U) Organizational Structure

(TS//SI//NF) NSA conducted all PSP analysis and reporting at its headquarters at Ft. Meade, Maryland, within the SIGINT Directorate. Specifically, tasking approvals, analysis, and reporting were conducted in the CT Product Line within SID, Analysis and Production. Collection of data was managed in SID, Directorate for Acquisition. No PSP activities were managed at NSA field sites.

[OIG will insert high level SID org chart from 2001 here]

(TS//SI//NF) Although the formal chain of command for SIGINT operations was through SID, in practice, the Director and Deputy Director of NSA/CSS managed the Program while keeping the SIGINT Director informed. Over time, the SIGINT Director became more involved, but the Director and Deputy Director always maintained direct operational control.

(TS//SI//NF) **Program Manager.** Five officials held the Program Manager position over the life of the PSP.[5] Initially, the Program Manager reported to the Chief of the CT Product Line. In 2004, the Program Manager position was restructured as the *SID Program Manager for CT Special Projects* and elevated to report to the SIGINT Director. This allowed the Program Manager jurisdiction of PSP elements across SID, not just those within the Directorate for Analysis and Production. At that time, the position was also formally designated as a senior level civilian position. A small staff was added to form the Program Management Office.

(TS//SI//NF) **SID Analysis and Production.** Initially, the MAC analyzed PSP metadata (data that describes the content, events, or networks associated with SIGINT targets), while SIGINT Development in the CT Product Line analyzed non-PSP metadata. The CT Product Line performed PSP content analysis. SIGINT Development, a separate organization within the SID, managed approvals for content tasking. In 2004, the analysis and production of metadata and content were consolidated into a new organization called the Advanced Analysis Division (AAD). AAD was divided into three teams: internet metadata, telephony metadata, and content.

(TS//SI//NF) **Coordination with FBI and CIA.** By 2004, four FBI integrees and two CIA integrees, operating under SIGINT authorities in accordance with written agreements, were co-located with NSA PSP-

[5](TS//SI//NF) The Chief of the CT Product Line was Acting Program Manager for a brief time in 2004.

cleared analysts. The purpose of co-locating these individuals was to improve collaborative analytic efforts.

(TS//SI//NF) **SID Data Acquisition.** Through the life of the Program, data collection was managed by Special Source Operations in SID, Data Acquisition Directorate. Collection managers were responsible for putting telephone numbers and email selectors on PSP-authorized collection by private sector companies and taking them off collection.

(U) Metadata

(TS//SI//NF) The authority to collect bulk telephony and Internet metadata significantly enhanced NSA's ability to identify activity that may have been terrorist-related. Contact chaining is the process of building a network graph that models the communication (e-mail, telephony, etc.) patterns of targeted entities (people, organizations, etc) and their associates from the communications sent or received by the targets.[6] Metadata is data that describes other data, specifically information that describes the content, events or networks associated with SIGINT targets. For example, for an email message, it would include the sender and recipient email addresses. It does not contain the subject line or the text of the email; they are considered to be content. Likewise, for a telephone conversation, metadata would include the called number and the calling number as well as the duration of the call.

(TS//SI//NF) Although NSA had the capability to collect bulk telephony and Internet metadata prior to the PSP, its application was limited because NSA did not have the authority to collect communications in which one end (the number being called or the recipient address of an e-mail) was in the United States. PSP significantly increased the data available to NSA analysts and allowed them to create more thorough contact chaining. This gave NSA the key to an early warning system—the ability to identify individuals in the United States or individuals outside the U.S. using U.S. telecommunications structures in contact with a foreign target, a terrorist.

(TS//SI//NF) Because metadata was not constitutionally protected, NSA did not consider it to be as sensitive as content collection. Nevertheless, processes were set up to document requests for metadata analysis and justifications for conducting such analysis under Program authority. The

[6] (TS//SI//OC/NF) Additional chaining can be performed on the associates' contacts to determine patterns in the way a network of targets may communicate. Additional degrees of separation from the initial target are referred to as "hops." For example a direct contact is one hop away from the target. A contact of the direct contact would be described as being 2 hops away from the target. The resulting contact-graph is subsequently analyzed for intelligence and to develop potential investigative leads.

following describes the process used to obtain requests, conduct analysis, and report results under the PSP. (See Appendix E for a flowchart of the end-to-end process.)

(TS//SI//NF) **Requests for Information and Leads.** Contact chaining analysis requests were received from FBI, CIA, or NSA. Requests typically took one of two forms, Requests for Information (RFI) and Leads. RFIs were specific questions about a target's telephone numbers or email addresses, called "selectors" at NSA. Leads were more general requests about a target's contacts. Requestors submitted leads to discover new investigative leads. Contact chaining requests were documented from the inception of the PSP.

(TS//SI//OC/NF) **Approvals to Chain.** Prior to chaining, NSA counterterrorism shift coordinators reviewed chaining requests to determine whether they met criteria provided by the OGC and based on the terms of the Authorization. They had to have enough information to identify a terrorism nexus and demonstrate compliance with criteria required by the Authorization before analysis could begin. Shift coordinators either approved requests, approved them for 1-hop (direct contact) analysis, or denied them. Approved requests were passed to analysts for contact chaining.

(TS//SI//OC/NF) **Analysis.** NSA used a variety of tools to conduct metadata analysis and view the results. NSA's primary tool for conducting metadata analysis, for PSP and traditional SIGINT collection, was MAINWAY. MAINWAY was used for storage, contact chaining, and for analyzing large volumes of global communications metadata. At the beginning of the PSP, only the "SIGINT Navigator" tool was available to view MAINWAY output. Over time, new tools and new processes, such as automated chaining alerting, were created to improve analysts' efficiency. To obtain the most complete results, analysts used data collected under PSP and non-PSP authorities. Typically, they analyzed networks with two degrees of separation (two hops) from the target. Analysts determined if resulting information was reportable.

(TS//SI//OC/NF) In addition, an automated chaining alert process was created to alert analysts of new potentially reportable selectors. Previously approved selectors were compared to incoming MAINWAY data authorized by the PSP, E.O. 12333, or the FISC. Alerts of direct contacts with approved selectors were reported to NSA analysts for further analysis and potential reporting to FBI and CIA.

WORKING DRAFT

(TS//SI//NF) **Storage.** NSA stored metadata obtained under PSP authorities in a protected database. Only cleared and trained analysts were given access to PSP metadata.

(TS//SI//OC/NF) **Reporting.** Reports based on metadata analysis were typically referred to as "tippers." Tippers contained contact chaining analysis results relevant to terrorism or with potential links to terrorism that warranted the attention of the FBI or the CIA for further investigation. Before releasing reports with U.S. person information, analysts obtained permission to do so in accordance with established NSA dissemination procedures.

(TS//SI//OC/NF) For each published report, NSA retained documentation of the analysis, supporting RFI or lead information, and a justification statement explaining the link to terrorism. If a report was not published, documentation was not retained. Counterterrorism personnel manually updated information in a computer tracking system to reflect the disposition of chaining requests.

(U) Content

(TS//SI//NF) Collection and analysis of content is NSA's traditional way of reporting ~~means of conducting~~ SIGINT. Content generally refers to words spoken during a telephone conversation or the written text of an email message. NSA collection of the content of telephony and Internet communications under the PSP improved its ability to produce intelligence on terrorist-related activity. For example, by allowing NSA access to links carrying communications with one end in the United States, NSA significantly increased its access to transiting foreign communications, i.e., with both communicants outside the United States. General Hayden described this as "the real gold of the Program." And, by allowing the intercept of international communications, NSA was able to identify threats within the United States.

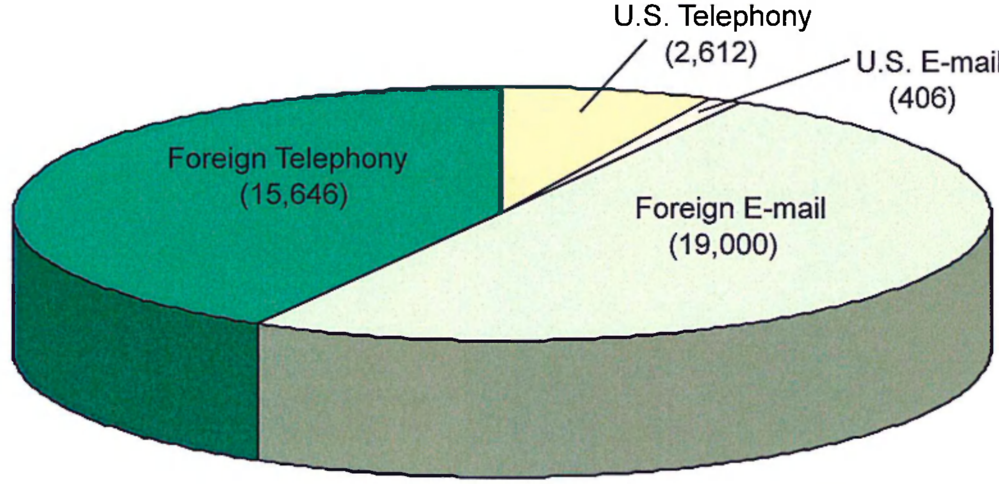
(TS//SI//NF) From the start of the Program until January 2007, NSA issued 490 reports based on PSP-derived content information. Also, as shown below, approximately 37,664 telephony and Internet selectors were tasked for
PSP-authorized content collection during that time period. Only 8 percent were U.S. targets. The vast majority
(92 percent) were foreign.

(TS//SI//OC/NF)

ST-09-0002
WORKING DRAFT

Approximate Number of Selectors Targeted for PSP Content Collection

4 Oct 2001 to 17 Jan 2007 *



(TS//SI//OC/NF)

(TS//SI//NF) NSA leadership considered selectors for targets located in the United States to be extremely sensitive. As such, processes were set up to ensure strict compliance with the terms of the Authorization. The following describes the general process for tasking, collecting, storing and reporting telephony and Internet content under the PSP. (See Appendix F for a flowchart of the end-to-end process.)

(TS//SI//STLW//NF) **Tasking Approvals.** Under the PSP, each domestic selector tasked for content collection was formally approved and tracked. Analysts submitted content collection requests, also called tasking packages, to the Chief of CT for approval. Tasking packages contained a narrative analysis, conclusion, supporting information, documentation, and a checklist of package contents. In the Chief's absence, the Deputy Chief of CT or the Program Manager could approve the requests. The approving officials reviewed the tasking packages to ensure that the proposed target and related metadata selectors met criteria in the Authorization. If criteria were not met, the officials requested additional information or denied the request. In limited cases, collection was approved for specific time periods. If the content contained foreign intelligence, the time period for collection would be extended. If it did not, collection was stopped. All approvals were documented in tasking packages.

WORKING DRAFT

(TS//SI//NF) Foreign selectors tasked for PSP content collection did not require formal approvals or tasking packages. Analysts were responsible for determining whether a foreign selector met the criteria for foreign intelligence ~~terms of the Authorization~~.

(TS//SI//NF) **Collection.** After a ~~domestic~~ selector was approved for PSP ~~content~~ collection, it was identified as "tasked" in the STELLARWIND Addresses Database by CT/AAD tasking managers who then emailed a collection tasking request to the SSO Collection Manager for telephony and Internet content collection. Foreign selector content collection requests were sent directly to the SSO Collection Manager. They did not require special approval.

(TS//SI//STLW//NF) SSO collection managers were responsible for ensuring that telephony and Internet content selectors were put on or taken off collection. For ~~telephony~~ telephony content selectors, collection managers sent content collection tasking instructions to private sector companies. Private sector companies were responsible for implementing tasking at front-end devices to obtain the required content collection. For Internet content selectors, collection managers sent content tasking instructions directly to equipment installed at company-controlled locations. Collected data was sent back to NSA/SSO and made available to analysts through the HYBRID voice processing system for telephony content selectors or the PINWALE database for Internet content selectors. SSO collection managers worked with private sector companies and the CT Product Line to ensure that collected data was as intended and legally authorized.

(TS//SI//NF) **Storage.** Content (voice or d~~D~~ata) collected under PSP was stored in protected partitions in existing NSA databases. Access to the partitions was restricted to PSP-cleared personnel.

(TS//SI//NF) **Reporting.** After analyzing content data collected under Presidential authority and identifying foreign intelligence information, counterterrorism analysts wrote reports. After an initial review within the CT Product Line, some reports were sent to SID Oversight and Compliance (O&C) for a second review for U.S. person identities. O&C reviewers determined whether the U.S. identities in the report were necessary to assess or understand the foreign intelligence information being reported or was required within the conduct of recipient's official duties. If an identity was found to be unnecessary, it was not reported. Before any U.S. person information was disseminated in reporting, internal NSA approvals were obtained as required by *United States Signals Intelligence Directive SP0018 – Legal Compliance and Minimization Procedures.*

(TS//SI//STLW//NF) Initially, NSA responded to FBI and CIA information requests in encrypted email. These initial reports, sometimes called "Tippers" or "Snippets," were "hidden in plain sight," meaning the information in the report did not reveal the source of the information. Later, FBI and CIA wanted to understand how NSA knew certain information that could not be provided in normal reporting channels. Eventually, "tear line" reporting was established. Tear lines are used regularly by NSA as a way to report SIGINT-derived information and sanitized information in the same report to appropriately cleared individuals. The sanitized "tear line" information conveys the same basic facts as the COMINT-controlled information while hiding COMINT as the source.

(TS//SI//NF) Dissemination of SIGINT Product

(TS//SI//NF) Regardless of which organization submitted requests or leads to NSA, all resulting reports were sent to CIA and FBI. Reports answered specific RFI questions or provided new investigative leads developed from chaining analysis. Reports contained selectors of interest (potential leads) with potential terrorist connections, not full chaining results. NSA had minimal insight into how CIA and FBI used PSP products.

(U) Discovery Requests

(U) On occasion, the Department of Justice (DoJ) attorneys determine that the facts of a particular matter justify a search of NSA files and submit a search request. In response to those requests or in response to discovery orders, NSA conducts a search of its databases to locate records that may fall within the scope of DoJ's discovery obligations and Rule 16 of the Federal Rules of Criminal Procedure. Typically the search process begins with a written request from DoJ including the names and aliases of individuals. NSA attorneys work with personnel trained in the retrieval of NSA reports to craft search strategies reasonably designed to identify reporting that may be responsive to the request. These search strategies are then used to perform electronic searches of NSA repositories of disseminated foreign intelligence reports. All responsive reports, to the extent any exist, are made available for review by DoJ.

(TS//SI) NSA searches only databases of reported intelligence and does not search databases containing acquired but not processed information (e.g., raw traffic) or acquired and processed but not reported or disseminated

WORKING DRAFT

information/communications (e.g., gists). NSA would include in its search applicable disseminated foreign intelligence derived from the PSP.

(TS//SI) After the search is completed, NSA provides all information, including PSP-derived material, to a small number of appropriately cleared DoJ individuals in the National Security Division who review the information on behalf of the DoJ and file motions on behalf of the government and the United States Attorney.

(U) Funding for NSA Activity Authorized by the PSP

(TS//SI//STLW//NF) NSA spent approximately $146,058,000 in CT supplemental funds for Program activities from FY02 through FY06. The funds were given annually to SID for Project MAINWAY hardware and contract support, analytic tools and contract analytic support, and collaborative partnerships with private sector companies. Funding requests were submitted annually to the PSP Program Manager and CT program budget officer. Each request had to justify why funds were needed and how the purchased item or service would support SID's PSP activities.

(TS//SI//STLW//NF) **Program Costs FY01 to FY06 ($ in thousands)**

Category	Description	FY02	FY03	FY04	FY05	FY06	Total
Data	Metadata and content (including one time set-up costs)	$25,668	$14,050	$15,500	$21,150	$25,900	$102,268
Tools and Systems	Processing, display and manipulations capabilities	$9,700	$8,000	$8,000	$9,500	$8,000	$43,200
Infrastructure	Facilities and equipment to support program	$590	0	0	0	0	$590
TOTALS		$35,958	$22,050	$23,500	$30,650	$33,900	$146,058

ST-09-0002
WORKING DRAFT

WORKING DRAFT

(U) THREE: ACCESS TO LEGAL REVIEWS, THE AUTHORIZATION, AND INFORMATION ABOUT THE PROGRAM

(U//FOUO) NSA did not have access to the original OLC legal opinion, but did have access and provided input to an OLC opinion prepared in 2004. The original Authorization and renewals were kept in the NSA Director's safe, and access to the documents was tightly controlled. By January 2007, nearly 3,000 people had been briefed on the PSP, including members of Congress and the FISC.

(U) Access to Legal Reviews

(TS//SI//NF) The NSA did not have access to the early DoJ Office of Legal Counsel (OLC) opinions supporting the Attorney General's statement that the PSP was legal. General Hayden, NSA lawyers, and the NSA Inspector General agreed that it was not necessary for them to see the early opinions in order to execute the terms of the Authorization, but felt it would be helpful to do so. NSA was, however, given access and provided comments to the OLC opinion issued in 2004.

(U) Access to OLC's Original Legal Review

(TS//SI//NF) Two NSA requests for access to the original OLC legal opinion were denied.

(TS//SI//NF) **First Request.** NSA General Counsel Robert Deitz stated that he asked the Vice President's Counsel if he could see the opinion. Even though Mr. Deitz's request was denied, the Vice President's Counsel read a few paragraphs of the opinion to him over the classified telephone line.

(TS//SI//NF) **Second Request.** At a 8 December 2003 meeting with the DoJ Associate Deputy Attorney General to discuss collection of metadata and an upcoming NSA OIG compliance audit, NSA's IG and Deputy GC requested to see the OLC legal opinion. The Counsel to the Vice President, who unexpectedly attended the meeting, denied the request and said that any request to see the opinion had to come directly from General Hayden.

(TS//SI//NF) General Hayden stated he never asked for or read the OLC legal opinion supporting the PSP. The Deputy GC stated that it was his

understanding that the opinion was not shared with NSA because it was considered confidential legal advice to the President.

(TS//SI//NF) The IG, GC, and Deputy GC agreed that their inability to read the OLC opinion did not prevent or impair them from executing and overseeing the Program. They were able to determine legality of the Program independently from DoJ (see Appendix D). However, the IG said that he found the secrecy surrounding the legal rationale to be "odd." Specifically, he said that it was "strange that NSA was told to execute a secret program that everyone knew presented legal questions, without being told the underpinning legal theory." The IG, GC, and Deputy GC all stated that they had yet to see the full text of the original OLC opinion.

(U//FOUO) Access to the May 2004 Opinion

(U//FOUO) In 2003 and 2004, the DoJ Associate Deputy Attorney General and the OLC Assistant Attorney General visited NSA to receive briefings on the PSP. On 04 May 2004, NSA, at the request of the OLC Assistant Attorney General, provided comments on the OLC's draft opinion on the Legality of the PSP. The OLC Assistant Attorney General submitted his opinion on 06 May 2004.

(U//FOUO) Access to the Presidential Authorization

(TS//SI//NF) As directed by the White House, access to the original Presidential authorization and subsequent renewals was tightly controlled.

(C) The Vice President's Counsel drafted the Authorizations and personally delivered them to NSA. On a few occasions, NSA picked up the Authorization at the White House.

(C) The first Authorization and subsequent renewals were kept in a safe in the Director's office. Initially, access was limited to General Hayden and a few others, including three OGC attorneys, Program Managers, and certain operational personnel. Those with access were not allowed to disseminate the Authorizations.

(TS//SI//NF) Importantly, most NSA operations personnel, including the Chief of the CT Product Line, who approved tasking for content collection, were not allowed to see the actual authorization. Rather, OGC answered targeting, information sharing, and implementation legal questions on an "on call" basis for operators. When the Authorization changed, OGC

WORKING DRAFT

summarized those changes in emails distributed to key program executives or communicated changes in due diligence meetings.

(TS//SI//OC/NF) Such limited access to the Authorization was documented in an IG investigation as a primary cause of two early violations of the Authorization. At the IG's recommendation, in March 2003, General Hayden began issuing Delegation of Authority letters that explained the Authorization as it applied to executing the Program. A new Delegation of Authority was promulgated with each renewal of the Authorization. The Delegation of Authority letters were sent to the Program Manager and the two managers of the SID CT Product Line and not further disseminated. (See Section Six.)

(U) Access to Program Information

(TS//SI//STLW//NF) Between 4 October 2001 and 17 January 2007, NSA cleared over 3,000 people for the PSP. The majority worked at NSA. Others were from the CIA, the FBI, the Department of Justice, Congress, the FISC, the ODNI, the White House, and the DoD.

(TS//SI//STLW//NF) **PSP Clearance Totals**

Agency	Number of Cleared Personnel
NSA	1,936
CIA	460
FBI	467
DOJ	64
Congress	60

FISC	14
ODNI	13
White House	14
DOD (excluding NSA)	5
Total	3,033

(TS//SI//STLW//NF) Within the first 30 days of the Program, over 190 people were cleared into the Program. This number included Senators Robert Graham and Richard Shelby, Congresswoman Nancy Pelosi, President George W. Bush, Vice President Richard Cheney, Counsel to the Vice President David Addington, and Presidential Assistant I. Lewis "Scooter" Libby. By 31 January 2002, FISC Judge Royce Lamberth was cleared. By June 2002, over 500 people had been cleared, including two additional members of Congress, Senator Daniel Inouye and former Senator Theodore Stevens, as well as FISC Judge Colleen Kollar-Kotelly. See Appendix G for a list, by date, of the number of people briefed into the Program.

(U) Non-Operational Personnel

(TS//SI-ECI//NF) Knowledge of the PSP was strictly limited at the express direction of the White House. General Hayden, over time, delegated his PSP clearance approval authority for NSA, FBI, and CIA operational personnel working the mission to the NSA PSP Program Manager. For members of Congress, FISC, outside counsel for providers, and the NSA IG, General Hayden had to obtain approval from the White House.

(U//FOUO) From the start, General Hayden and NSA leadership pushed to keep members of the legislative and judicial branches of government informed. General Hayden said he told the Vice President that he had no

WORKING DRAFT

concerns about the lawfulness of the Authorization but worried about the politics. After some hesitancy, the White House gave General Hayden permission to brief certain members of Congress. In addition, the Chief Judge of the FISC was first cleared in January 2002 (see Section ____).

(TS//SI//NF) **Interactions with Members of Congress.** Between 25 October 2001 and 17 January 2007, General Hayden, sometimes supported by operational target experts from the CT Product Line and SSO office, conducted over 49 briefings to members of Congress or their staff. (See Appedix __ for a complete list of briefings.)

(TS//SI//NF) General Hayden first briefed the following members of Congress on 25 October 2001:

- Chair - House Permanent Select Committee on Intelligence
- Ranking Minority Member of the House Permanent Select Committee on Intelligence
- Chair – Senate Select Committee on Intelligence
- Vice Chair – Senate Select Committee on Intelligence

(TS//SI//NF) In addition, NSA received and responded to a variety of Program-related inquiries from members of Congress, including Senators Inouye, Stevens, Pelosi, and Rockefeller.

(U//FOUO) General Hayden always believed that the PSP was legal. He said that during the many PSP-related briefings he gave to members of Congress, no one ever said that NSA should stop what it was doing. He emphasized that he did not just "flip through slides" during the briefings. They lasted as long as attendees desired.

(TS//SI//NF) **Interactions with the FISC.** On 31 January 2002, Chief Judge Royce Lamberth was briefed on the PSP and on 17 May 2002, his successor, Colleen Kollar-Kotelly, was briefed. A law clerk was also briefed in April 2004. (See Section Five.)

(U//FOUO) The Clearance Process

(TS//SI-ECI//NF) NSA managed the NSA clearance process. Clearance requests were submitted to the PSP Program Office for Program Manager approval or disapproval. Access was granted only to those who needed it

to perform assigned job duties. The Program Manager questioned access requests with unclear justifications. Approved requests were forwarded to the Program security officer, who performed a security check. If the security check yielded nothing to impede access, individuals were instructed to go to the security office to read the "Security Pre-Brief Agreement" and sign a "Sensitive Compartmented Information Nondisclosure Agreement" form. NSA's General Counsel also had the authority to read in Attorneys from other agencies.

(TS//SI//NF) On 20 May 2005, the Program Manager changed the PSP clearance request and re-certification process. The Project Security Officer assigned to Special Source Operations in the SIGINT Directorate assumed responsibility for the PSP clearance process. (Special Source Operations managed all PSP-related collection for NSA.) Additionally, the Program Manager initiated monthly PSP clearance briefings.

(TS//SI//NF) From 4 October 2001 until 23 May 2005, a two-level PSP clearance structure was used. One level was limited to the "fact of" Program existence. A second level included access to PSP targeting data through a "must know" principle. Access lists were maintained in the SSO Security Director's office on an internal SSO compartmented LAN.

(TS//SI-ECI//NF) Regular zero-based reviews were conducted by the SSO Security Director's office quarterly to validate that cleared individuals had a continuing need for access to PSP information. The clearance did not automatically transfer with individuals who moved to new assignments. The clearance had to be re-justified for the new position, or the individual would be debriefed from the Program.

WORKING DRAFT

(U) FOUR: NSA PRIVATE SECTOR RELATIONSHIPS

(TS//SI//NF) To conduct foreign intelligence-gathering activities under the PSP, NSA required the assistance of private companies, which provided access to international communications chokepoints in United States. Immediately after 11 September 2001, some private companies contacted NSA to offer support. Subsequent to PSP authorization, NSA sent request letters to companies stating that their assistance was authorized by the President with legal concurrence of the Attorney General.

(U) Need for Private Sector Cooperation

(TS//SI//NF) The United States carries out foreign intelligence activities through a variety of means. One of the most effective means is to partner with commercial entities to obtain access to information that would not otherwise be available.

(U//FOUO) Telephony

(TS//SI//NF) Most international telephone calls are routed through a small number of switches or "chokepoints" in the international telephone switching system en route to their final destination. The United States is a major crossroads for international switched telephone traffic. For example, in 2003, circuit switches worldwide carried approximately 180 billion minutes of telephone communications. Twenty percent of this amount, over 37 billion minutes, either originated or terminated in the United States, and another thirteen percent, over 23 billion minutes, transited the United States (neither originating nor terminating here). [NSA is authorized under Executive Order 12333 to acquire transiting telephone calls.]

(TS//SI//NF) NSA determined that under the Authorization it could gain access to approximately 81% of the international calls into and out of the United States through three corporate partners: COMPANY A had access to 39%, COMPANY B 28%, and COMPANY C 14%. NSA did not seek assistance from local exchange carriers, because that would have given NSA access primarily to domestic calls.

(U//FOUO) Internet Communications

(TS//SI//NF) Al Qaeda and associated terrorist organizations have made extensive use of the Internet. It is their preferred method of communication. Terrorists use Internet communications, particularly web-based services, because they are ubiquitous, anonymous, and usually free of charge. They can access Web-based email accounts and similar services from any origination point around the world.

(TS//SI//NF) The United States is a major Internet communications hub. The industry standard for characterization of the volume of Internet communications is bandwidth, which measures the amount of digital data transmitted in one second – bits per second or bps. For example, data available from 2002 shows that at that time, worldwide international bandwidth was slightly more than 290 Gbps[7]. Of that total, less than 2.5 Gbps was between two regions that did not include the United States.

(TS//SI//NF) The United States is also home to computer servers providing Internet communications services often used by terrorists. The majority of known terrorist email addresses that NSA has tracked are hosted on U.S.-based providers or foreign-managed providers hosted on servers in the United States. (e.g. [redacted].

(U//FOUO) Evolution of NSA Partnerships with Private Sector

(U) History of NSA Partnerships with Private Sector

(TS//SI//NF) As far back as World War II, NSA has had classified relationships with carefully vetted U.S. companies that assist with essential foreign intelligence-gathering activities. NSA maintains relationships with over 100 U.S. companies. Without their cooperation, NSA would not be able respond to intelligence requirements on a variety of topics important to the United States.

(TS//SI//NF) Two of the most productive SIGINT collection partnerships that NSA has with the private sector are with COMPANY A and COMPANY B. These two relationships enable NSA to access large volumes of foreign-to-foreign communications transiting the United States

[7](U) Gpbs is an abbreviation for Gigabits per second, which can also be described as one billion bits per second or 1,000,000,000 bps.

through fiber-optic cables, gateway switches, and data networks. They also provide foreign intelligence authorized under the FISA.

(TS//SI//NF) According to General Alexander, General Hayden's replacement as Director of NSA/CSS, if the relationships with these companies were ever terminated, the U.S. SIGINT system would be irrevocably damaged, because NSA would have sacrificed America's home field advantage as the primary hub for worldwide telecommunications.

(U) Partnerships after 11 September 2001

(TS//SI//NF) According to the former Deputy Chief of SSO, between 11 September 2001 and the 4 October 2001 Authorization, COMPANY A and COMPANY B contacted NSA and asked "what can we do to help?" COMPANY B personnel approached NSA SSO personnel through an existing program. They said they noticed odd patterns in domestic calling records surrounding the events of 11 September and offered call records and analysis. With no appropriate authority under which to accept the call records, NSA suggested the company contact the FBI.

(U//FOUO) Partnerships Supporting the PSP

(TS//SI//NF) Once the Authorization was signed on 4 October 2001, NSA began a process of identifying and visiting commercial entities requesting their support. While requesting help from corporate entities to support the PSP, NSA personnel made it clear that the PSP was a cooperative program and participation was voluntary. NSA knew that the PSP was an extraordinary program and understood if companies viewed it as too much of a liability.

(TS//SI//NF) NSA Approaches to Private Sector Companies

(TS//SI//NF) **2001:** On Columbus Day, 8 October 2001, NSA Special Source Operations (SSO) personnel responsible for the access relationships with corporate partners COMPANY A, COMPANY B, and COMPANY C were called in to work and informed that the President had authorized the PSP on 4 October 2001. The SSO personnel were tasked with initiating a dialog with the respective TS/SCI-cleared officials from COMPANIES A, B, and C to seek their cooperation under the new Authorization. Over the next few business days, SSO personnel met separately with officials from the three companies. Each company agreed to cooperate.

(TS//SI//NF) Upon confirmation that formal NSA letters requesting their assistance were forthcoming, the providers, acting independently and officially unaware of the cooperating agreements with other companies, initiated collection to support the PSP.

(TS//SI//NF) **2002:** In early 2002, NSA SSO personnel met with the Senior Vice President of Government Systems and other employees from COMPANY E. Under the authority of the PSP, NSA asked COMPANY E to provide call detail records (CDR) in support of security for the 2002 Olympics in Salt Lake City. On 11 February 2002, the company's CEO agreed to cooperate with NSA. On 19 February 2002, COMPANY E submitted a written proposal that discussed methods it could use to regularly replicate call record information stored in a COMPANY E facility and potentially forward the same information to NSA. Discussions with COMPANY E continued in 2003. However, the COMPANY E General Counsel ultimately decided not to support NSA.

(TS//SI//NF) On 5 September 2002, NSA legal and operational personnel met with internet provider COMPANY D's General Counsel to discuss the PSP and ask for the company's support. COMPANY D provided support, but it was minimal. (For a description of COMPANY D's support, see page __, "What Providers Furnished.").

(TS//SI//NF) On 29 October 2002, NSA legal and operational personnel met with internet provider COMPANY F's Legal and Corporate Affairs personnel, and a former NSA OGC employee hired by COMPANY F as independent counsel. NSA requested COMPANY F's support under the PSP for email content. At the meeting, COMPANY F requested a letter from the Attorney General certifying the legality of the PSP. In December 2002, NSA's Commercial Technologies Group was informed that the company's CEO agreed to support the PSP. According to NSA's General Counsel, COMPANY F did not participate in the PSP because of corporate liability concerns.

(TS//SI//NF) **2003:** In April 2003, NSA legal and operational personnel met with the President and Chief Operating Officer, General Counsel, and other personnel from private sector COMPANY G. After the meeting, the company's General Counsel wanted to seek the opinion of outside counsel. NSA determined the risk associated with additional disclosure outweighed what COMPANY G would have provided. NSA decided to not pursue a partnership with this company.

WORKING DRAFT

(U//FOUO) NSA Letters to Private Sector

(TS//SI//NF) The Director sent letters to private sector companies requesting their assistance with the PSP. NSA OGC drafted the letters for the Director, tracked each renewal of the President's authorization and modified the letters accordingly, and ensured the letters were delivered to the companies. Between 16 October 2001 and 14 December 2006, NSA sent 147 request-for-assistance letters to private sector partners.

- COMPANY A: 44 Letters
- COMPANY B: 44 Letters
- COMPANY C: 46 Letters
- COMPANY D: 11 Letters
- COMPANY E: 2 Letters

(TS//SI-ECI//NF) **2001.** In his first PSP-related letter on 16 October 2001 to COMPANIES A, B and C, General Hayden stated that the National Security Agency and the Federal Bureau of Investigation required their assistance "to collect intelligence vital to the national security arising from the events of 11 September 2001," and specifically requested that they "provide survey, tasking and collection against international traffic, some of which terminates in the United States; provide aggregated call record information; and supply computer to computer data which can be used to determine the communicants." Their assistance was "needed to identify members of international terrorist cells in the United States and prevent future terrorist attacks against the United States." These first letters also stated that the requested assistance was authorized by the President with the legal concurrence of the Attorney General, pursuant to Article II of the Constitution.

(TS//SI-ECI//NF) **2002:** Subsequent letters were sent to COMPANIES A, B, and C by General Hayden (or his deputy) each time the President reauthorized the PSP. Throughout 2002, these written requests for assistance referenced the 16 October letter; repeated the need to provide the Presidentially-authorized assistance; emphasized that such assistance was necessary to counter a future terrorist attack; and stated that such assistance was reviewed by the Attorney General and had been determined to be a lawful exercise of the President's powers as Commander-in-Chief. Starting in mid-2003, the wording of the letters was revised but in substance remained the same.

(TS//SI-ECI//NF) Two request letters for assistance were sent to private sector COMPANY E. The first letter was sent on 26 February 2002, and

the last letter was sent on 14 March 2002. All letters were signed by General Hayden.

(TS//SI-ECI//NF) In addition to the letters sent to COMPANY A, COMPANY B, COMPANY C and COMPANY E, eleven request letters for assistance were prepared for internet provider COMPANY D. The first letter was on 9 October 2002 and the last letter was 11 September 2003. All letters were signed by General Hayden or his designee.

(TS//SI-ECI//NF) **2003:** In June 2003, COMPANY C's General Counsel and Chief of Staff requested a written Attorney General opinion on the legality and lawfulness of the PSP, to include a directive to comply. COMPANY C cited corporate liability concerns as their reason. On 8 August 2003, the Attorney General sent COMPANY C a letter stating that the request for support was a lawful exercise of authorities assigned to the President under Article II of the Constitution. Additionally, the Attorney General directed COMPANY C to comply with NSA's request.

(TS//SI-ECI//NF) **2004:** On 26 March 2004, the President amended his 11 March 2004 authorization after deciding to discontinue bulk collection of Internet metadata. Before 11 March 2004, all authorizations covering Internet metadata collection (as well as content collection and telephony metadata collection) were approved for form and legality by the Attorney General. Accordingly, NSA's 12 March 2004 letters to the companies stated that the most recent authorization had been approved for form and legality by the Counsel to the President, not the Attorney General as with previous authorizations.

(TS//SI//ECI//NF) **2005:** Beginning 19 September 2005 through 14 December 2006, new NSA/CSS Director General Alexander, or his designee, signed the request letters to the companies.

(TS//SI-ECI//NF) **2006 Attorney General Letters.** On 24 January 2006, the Attorney General sent letters to COMPANIES A, B, and C, certifying under 18 U.S.C. 2511(2)(a)(ii)(B) that "no warrant or court order was or is required by law for the assistance, that all statutory requirements have been met, and that the assistance has been and is required."

(TS//SI-ECI//NF) **2006 DNI Letters.** On 13 April 2006, the Director of National Intelligence (DNI) sent letters to Companies A, B, and C to underscore the continuing critical importance of their assistance. The DNI letter also stated that the "intelligence obtained from their assistance has been and continues to be indispensable to protecting the country and the American people from terrorist attacks."

(TS//SI-ECI//NF) Letters for COMPANIES A, B, C, and E were couriered to the companies' local facility. COMPANY B sometimes picked up its letters at NSA Headquarters. Letters for COMPANY D were stored at NSA since no one at the company had the proper clearance to store them.

(U//FOUO) PSP Authorized Support to NSA

(TS//SI-ECI//NF) Private sector companies provided assistance to NSA under the PSP in three categories: telephone and Internet Protocol content, Metadata from Call Detail Records, and Internet Protocol Metadata.

(TS//ECI//NF) The PSP allowed content to be collected if the selected communication was one-end foreign or the location of the communicants could not be determined. Selectors (email addresses and telephone numbers) were provided by NSA's Office of Counterterrorism.

(TS//SI-ECI//NF) **Content: Telephony.** Under the PSP, companies provided the content of one-end-foreign international telephone calls (telephony content) and the content of electronic communications (email content) of al Qaeda and its affiliates. COMPANIES A, B, and C provided telephony content from communications links they owned and operated. They had been providing telephony content to NSA before 2001 under FISA and E.O. 12333 authorities. NSA began to receive telephony content from COMPANIES A and B on 6 October 2001 and COMPANY C on 7 October 2001. This support ended on 17 January 2007.

(TS//SI-ECI//NF) **Content: Internet Email.** COMPANIES A, B, and C provided access to the content of Al Qaeda and Al Qaeda-affiliate email from communication links they owned and operated. NSA received email content from COMPANY A as early as October 2001 until 17 January 2007, from Company B beginning February-March 2002 through 17 January 2007, and from COMPANY C from April 2005 until 17 January 2007. From April 2003 through November 2003, COMPANY D provided a limited amount of email content under the PSP. It did not provide PSP-related support after November 2003, but it did provide support under FISA.

(TS//SI-ECI//NF) **Metadata from Call Detail Records.** COMPANIES A and B provided Call Detail Records to NSA. The records were used by NSA Counter-Terrorism metadata analysts to perform call chaining and network reconstruction between known al Qaeda and al Qaeda-affiliate telephone numbers and previously unknown telephone numbers with which they had been in contact. Providers generated Call Detail Records as a normal course of doing business (e.g., billing purposes and traffic

engineering). Records included all call events from the companies' long distance and international communication networks. The Call Detail Records were aggregated as large files by TS/SCI-cleared groups at COMPANY A and COMPANY B and forwarded, on an hourly or daily basis, across classified communications circuits to a PSP-restricted NSA data repository.
COMPANY A provided PSP-authorized CDRs as early as November 2001, and COMPANY B began to provide CDRs in February 2002. Both continued to provide this support through the end of the PSP, and support continues today under the FISC Business Records Order. COMPANY C provided select PSP-authorized CDRs from December 2002 through March 2003.

(TS//SI-ECI//NF) **Internet Metadata**. The last category of private sector assistance was access to Internet Protocol (IP) metadata associated with communications of al Qaeda (and affiliates) from data links owned or operated by COMPANIES A, B, and C. In order to be a candidate for PSP IP metadata collection, data links were first vetted to ensure that the preponderance of communications was from foreign sources, and that there was a high probability of collecting al Qaeda (and affiliate) communications. NSA took great care to ensure that metadata was produced against foreign, not domestic, communications.

(TS//SI-ECI//NF) COMPANY A began providing PSP IP metadata collection as early as November 2001. Although COMPANY B began providing CD-ROMs of PSP IP metadata in October 2001, an automated transfer of data was not available until February-March 2002. The Presidential authority to collect IP metadata was terminated in March 2004. COMPANY A and COMPANY B IP metadata collection resumed after the FISC Pen Register/Trap & Trace (PR/TT) Order authorizing this activity was signed on 15 July 2004. COMPANY C provided IP metadata beginning in April 2005.

WORKING DRAFT

This page intentionally left blank.

ST-09-0002
WORKING DRAFT

(U) FIVE: NSA'S INTERACTION WITH THE FISC AND TRANSITION TO COURT ORDERS

(TS//SI//NF) Until 2006, NSA's PSP-related interaction with members of the FISC was limited to informational briefings to the Chief Judge. Chief Judge Royce Lamberth, Judge Colleen Kollar-Kotelly, who replaced Judge Lamberth as Chief Judge in May 2002, and one law clerk were the only members of the FISC that NSA had briefed on the PSP In the spring of 2004, NSA's interaction with Judge Kollar-Kotelly increased as NSA and DoJ began transitioning PSP-authorized activities to FISC orders in 2004. It was not until after parts of the PSP were publicly revealed in December 2005 that all members of the FISC were briefed on the Program.

(U) NSA's Interaction with the FISC

(TS//SI//NF) General Hayden stated that from the start of the PSP, he and other NSA leaders recognized the importance of keeping all three branches of the Government informed of the Program and pressed the White House to do so.

(TS//SI//NF) In all of its interactions, neither NSA nor DoJ presented before the FISC the factual and legal issues arising from the PSP in any case or controversy. Therefore, the FISC did not express any view or comment on the legality or illegality of the PSP.

(U//FOUO) NSA Briefings on the PSP to Members of the FISC

(TS//SI//NF) The White House first permitted NSA to brief the Chief Judge of the FISC in January 2002. General Hayden stated that on 31 January 2002, he provided Judge Lamberth a very detailed PSP briefing, and the Deputy Assistant Attorney General in the DoJ OLC explained the Program's legality. General Hayden stated that this briefing was prompted by a concern expressed by DOJ that PSP-derived information would be used in FISA applications

(TS//SI//NF) On 17 May 2002, General Hayden briefed incoming Chief Judge Kollar-Kotelly, with Judge Lamberth in attendance, on the PSP. In a

letter to the Counsel for Intelligence Policy dated 12 January 2005, Judge Kollar-Kotelly stated that, on that date, she was also shown a short legal memorandum, prepared by the Deputy Assistant Attorney General in the DoJ, OLC, that set out a broad overview of the legal authority for conducting the PSP. Judge Kollar-Kotelly added that she was allowed to read the memorandum but not to retain it for study.

(TS//SI//NF) NSA records show that Judge Kollar-Kotelly was briefed again on 12 August 2002 at the White House. Although we found no documentation of the purpose of the meeting or topics discussed, Judge Kollar-Kotelly stated in the January 2005 letter to the Counsel for Intelligence Policy that, at her request, she was permitted to review the Authorization of the PSP on that date.

(TS//SI//NF) In response to a *New York Times* "warrantless wiretapping" story published in December 2005, General Alexander briefed all FISC members on the PSP on 9 January 2006.[9]

(U) Transition of PSP Authorities to FISC Orders

(TS//SI//NF) The transition of PSP-authorized activities to FISC orders was precipitated by preliminary results of DoJ OLC legal review of the components of the Program. In March 2004, OLC found three of the four types of collection authorized under the PSP to be legally supportable. However, it determined that, given the method of collection, bulk Internet metadata was prohibited by the terms of FISA and Title III.[10] Consequently, the White House Counsel rather than the Attorney General signed the 11 March 2004 Authorization.

(TS//SI//NF) NSA Implements Controversial 11 March 2004 Authorization

[9] (TS//STLW//SI//OR/NF)Judge Scullin did not attend this briefing, but was later briefed on 31 January 2006. Judge Bates, a new judge, was briefed on 21 March 2006.

[10](TS//STLW//SI//OR/NF) OLC ultimately issued three opinions: 15 March 2004, 6 May 2004, and 16 July 2004.

ST-09-0002
WORKING DRAFT

> *(TS//SI//NF) Until March 2004, NSA considered its collection of bulk Internet metadata under the PSP to be legal and appropriate. Specifically, NSA leadership, including OGC lawyers and the IG, interpreted the terms of the Authorization to allow NSA to obtain bulk Internet metadata for analysis because NSA did not actually "acquire" communications until specific communications were selected. In other words, because the Authorization permitted NSA to conduct metadata analysis on selectors that met certain criteria, it implicitly authorized NSA to obtain the bulk data that was needed to conduct the metadata analysis.*
>
> *(TS//SI//NF) On 11 March 2004, General Hayden had to decide whether NSA would execute the Authorization without the Attorney General's signature (IV-A/32-11). General Hayden described a conversation in which David Addington asked, "Will you do it (IV-A/32-11)?" At that time, General Hayden also said that he asked Daniel Levin, Counsel to the Attorney General, in March 2004 if he needed to stop anything he was doing. Mr. Levin said that he did not need to stop anything (IV-A/32-7 and IV-A/32a-7&8). After conferring with NSA operational and legal personnel, General Hayden stated that he decided to continue the PSP because 1) the members of Congress he briefed the previous day, 10 March, were supportive of continuing the Program, 2) he knew the value of the Program, and 3) NSA lawyers had determined the Program was legal.*

(TS//SI//NF) Eight days later on 19 March 2004, the President rescinded the authority to collect bulk Internet metadata and gave NSA one week to stop collection and block access to previously collected bulk Internet metadata. NSA did so on 26 March 2004. To close the resulting collection gap, DoJ and NSA immediately began efforts to recreate this authority in what became the PR/TT order. By January 2007, the remaining three authorities had also been replicated in FISC orders: the Business Records (BR) Order, the Foreign Content Order, and the

WORKING DRAFT

Domestic Content Order. On 1 February 2007, the final Authorization was allowed to expire and was not renewed.

(TS//SI//NF) Transition of Internet Metadata Collection to Pen Register/Trap and Trace Order Authority

(TS//SI//NF) According to NSA personnel, the decision to transition Internet metadata collection to a FISC order was driven by DoJ. At a meeting on 26 March 2007, DoJ directed NSA representatives from OGC and SID to find a legal basis, using a FISC order, to recreate NSA's PSP authority to collect bulk Internet metadata.

(TS//SI//NF) After extensive coordination, DoJ and NSA devised the PR/TT theory to which the Chief Judge of the FISC seemed amenable. DoJ and NSA worked closely over the following months, exchanging drafts of the application, preparing declarations, and responding to questions from court advisers. NSA representatives explained the capabilities that were needed to recreate the Authority, and DoJ personnel devised a workable legal basis to meet those needs. In April 2004, NSA briefed Judge Kollar-Kotelly and a law clerk because Judge Kollar-Kotelly was researching the impact of using PSP-derived information in FISA applications. In May 2004, NSA personnel provided a technical briefing on NSA collection of bulk Internet metadata to Judge Kollar-Kotelly. In addition, General Hayden said he met with Judge Kollar-Kotelly on two successive Saturdays during the summer of 2004 to discuss the on-going efforts.

(TS//SI//NF) The FISC signed the first PR/TT order on 14 July 2004. Although NSA lost access to the bulk metadata from 26 March 2004 until the order was signed, the order essentially gave NSA the same authority to collect bulk Internet metadata that it had under the PSP, except that it specified the datalinks from which NSA could collect, and it limited the number of people that could access the data. The FISC continues to renew the PR/TT approximately every 90 days.

(TS//SI//NF) Transition of Telephony Metadata Collection to the Business Records Order

(TS//SI//NF) According to NSA General Counsel Vito Potenza, the decision to transition telephony metadata to the Business Records Order was driven by a private sector company. After the *New York Times* article was published in December 2005, Mr. Potenza stated that one of the PSP providers expressed concern about providing telephony metadata to NSA under Presidential Authority without being compelled. Although OLC's

ST-09-0002
WORKING DRAFT

May 2004 opinion states that NSA collection of telephony metadata as business records under the Authorization was legally supportable, the provider preferred to be compelled to do so by a court order.[11]

(TS//SI//NF) As with the PR/TT Order, DoJ and NSA collaboratively designed the application, prepared declarations, and responded to questions from court advisers. Their previous experience in drafting the PRTT Order made this process more efficient.

(TS//SI//NF) The FISC signed the first Business Records Order on 24 May 2006. The order essentially gave NSA the same authority to collect bulk telephony metadata from business records that it had under the PSP. And, unlike the PRTT, there was no break in collection at transition. The order did, however, limit the number of people that could access the data and required more stringent oversight by and reporting to DOJ. The FISC continues to renew the Business Records Order every 90 days or so. (See Appendix H.)

(TS//SI//NF) Transition of Internet and Telephony Content Collection to the Foreign and Domestic Content Orders

(TS//SI//NF) According to NSA OGC, the transition of PSP content collection to FISC orders was driven by DoJ. DoJ had contemplated a transition in July 2004 when the FISC's signing of the PR/TT order indicated its willingness to authorize PSP activities under court order. Given this precedent, DoJ concluded the FISC might also accept content collection. However, little progress was made until June 2005 when the DoJ OIPR with NSA OGC and SID representatives began researching the feasibility of collecting PSP content under court order. In essence, DOJ and NSA needed to find a legal theory that would allow NSA to add and drop thousands of foreign targets for content collection. Because the law was more restrictive for content than metadata, NSA had serious reservations about whether it would be possible to find a workable solution using a FISC order at that time, especially given the large number of selectors to be tasked and the complexity from legal and operational perspectives. For example:

[11](TS//STLW//SI//OR/NF) In addition to the telephony metdata that NSA was receiving from private sector companies as business records, it was also obtaining "live" telephony metadata from its own SIGINT collection sources. It continued until mid-2005. (***We will include a reference to the corresponding notification here.***)

WORKING DRAFT

- ☒ (TS//SI//NF) NSA risked losing flexibility in the means of collection, given that facilities and collection accesses were complex and in constant flux.

- ☒ (TS//SI//NF) In executing the PR/TT and Business Records Orders, the FISC's and DoJ's consistently increasing demands for information took NSA analysts away from target-related duties.

- ☒ (TS//SI//NF) The process imposed by the FISA statute was not able to handle the large volume of NSA requests for FISC authorization needed after
11 September 2001.

- ☒ (TS//SI//NF) Because OLC's May 2004 opinion found that the existing Authorization for content collection was lawful, there was no pressing need to find an alternative legal vehicle.

(TS//SI//NF) In a letter dated 21 February 2006, the NSA GC expressed the aforementioned concerns, among others, to the Acting Assistant Attorney General suggesting that:

> " . . . . now might be the right time to seek substantial revisions to the FISA. The purpose of the legislation was to protect the privacy of U.S. persons who could be subjected to surveillance, either intentionally or incidentally. Twenty-seven years later, the United States Government finds itself obtaining FISA orders so that it can carry out surveillance on foreign intelligence targets who are outside the United States and, more often than not, communicating only with others outside the United States. This serves no U.S. person's privacy interests, was never anticipated by the statute's drafters, and diverts valuable resources from the fight against terrorism. The FISA needs to be simplified and streamlined."

(TS//SI//NF) Ultimately, DoJ decided to pursue a FISC order for content collection wherein the traditional FISA definition of a "facility" as a specific telephone number or email address was changed to encompass the gateway or cable head that foreign targets use for communications. Minimization and probable cause standards would then be applied. As with the PRTT and Business Records orders, NSA collaborated with DoJ to prepare the application and declarations and provided the operational requirements needed to continue effective surveillance.

(TS//SI//NF) After 18 months of concerted effort and coordination, the FISC ultimately accepted the theory for foreign selectors but rejected it for

domestic selectors. Consequently, on 10 January 2007, the FISC signed two separate orders: the Foreign Content Order and the Domestic Content Order.

(TS//SI//NF) The Foreign Content Order negatively affected SIGINT exploitation. Most notably, the number of foreign selectors on collection dropped by 73 percent, from 11,000 selectors under PSP to 3,000 under the order. In addition, the administrative workload for NSA analysts to put critical foreign selectors on collection was so burdensome that the order became operationally unsustainable. The order was eventually superseded by Congress' FISA modernization. It was temporarily replaced by the Protect America Act in August 2007 and then permanently replaced by the FISA Amendments Act in July 2008.

(TS//SI//NF) The Domestic Content Order did not create a similar loss in collection because so few domestic numbers were tasked at that time. It did, however, slow operations because of the documentation required, and it took considerably longer to task under the order than under the PSP. Over time, the scope of the Domestic Content Order gradually decreased to a single selector tasked for collection in January 2009. In January 2009, the FBI, at NSA's request, assumed responsibility for the Domestic Content Order and became the declarant before the FISC.

WORKING DRAFT

(U) SIX: NSA OVERSIGHT OF PSP SIGINT ACTIVITIES

(U//FOUO) NSA Office of General Counsel and SID, Oversight and Compliance provided oversight of NSA PSP activities from October 2001 until January 2007. NSA OIG initiated PSP oversight in 2002.

(U) Office of General Counsel

(U//FOUO) The OGC was the first NSA organization with oversight responsibilities to learn of the PSP, and it continued to provide significant oversight over the life of the Program. The GC was briefed on 4 October 2001, the day the Authorization was signed. On 6 October, he gave the Director and Deputy Director talking points for briefing NSA personnel on the new authority. The talking points included the fact that General Hayden had instructed the GC and the lead attorney for operations to conduct routine review and oversight of PSP activities.

(U//FOUO) The NSA Assistant General Counsel for Operations provided most of the Program oversight before the OIG learned of the PSP in 2002. He and his successors reviewed proposed target packages and rejected those not compliant with the Authorization, answered questions, gave briefings, reviewed program implementation, and coordinated program-related issues with DoJ.

(U) SIGINT Directorate

(U//FOUO) The SIGINT Directorate Office of Oversight and Compliance (O&C) represents the Director NSA/CSS and the Signals Intelligence Director in overseeing compliance with authorities that govern the collection, production, and dissemination of intelligence by the National Security Agency. The Chief of O&C was briefed on the PSP on 10 October 2001. Initially, O&C's ability to provide effective oversight was limited by insufficient staffing and a lack of methodologies to provide meaningful oversight of PSP collection. It, therefore, focused on identifying problem areas while documenting program activity. It also helped establish database partitions and assisted with data flow compliance issues to prevent uncleared personnel from seeing Presidentially-authorized collection. Later, it reviewed justification statements for tasked selectors. Also, it directed PSP-cleared SIGINT operations personnel to follow

established procedures for the dissemination of U.S. person information and obtained approvals to permit dissemination of U.S. person information

(U) Office of Inspector General

(U//FOUO) NSA OIG conducted oversight of PSP activities from August 2002 until the Program ended in January 2007. It issued 12 formal reports and 14 Presidential Notifications on PSP activities at NSA.

- (U) **Investigations** were conducted in response to specific incidents or violations to determine the cause, effect, and remedy.
- (U) **Reviews** were conducted to determine the adequacy of management controls to ensure compliance with the Authorization and related authorities; to assess the efficiency and effectiveness in mitigating high-risk activities associated with the Program; and to identify impediments to satisfying the requirements of the Authorization and related authorities.
- (U) **Presidential Notifications** were drafted for the Director's signature to notify the President's Counsel about violations of the Authorization. (See below for additional details.)
- (U) **Monthly Due Diligence Meetings** were held by program officials to exercise "due diligence" in addressing program issues and developments. The OIG attended these meetings to stay aware of program activities.

(U//FOUO) OIG also provided oversight of FISC-authorized activity previously conducted under Authorization.

(U//FOUO) See Appendix H for a list of OIG reports on PSP activity at NSA.

WORKING DRAFT

(U) NSA IG Not Cleared until 2002

(TS//SI//NF) We could not determine exact reasons for why the NSA IG was not cleared for the PSP until August 2002. According to the NSA General Counsel, the President would not allow the IG to be briefed sooner. General Hayden did not specifically recall why the IG was not brought in earlier, but thought that it had not been appropriate to do so when it was uncertain how long the Program would last and before operations had stabilized. The NSA IG pointed out that he did not take the IG position until April 2002, so NSA leadership or the White House may have been resistant to clearing either a new or an acting IG.

(TS//SI//NF) Regardless, by August 2002, General Hayden and the NSA General Counsel wanted to institutionalize oversight of the Program by bringing in the IG. General Hayden recalled having to "make a case" to the White House to clear the IG at that time.

(U//FOUO) OIG concerns lead to change

(C) In addition to formal recommendations made in review and investigative reports, OIG concerns about access to the terms of the Presidential authorization and about the means of reporting PSP violations resulted in three major changes.

(C) First, in December 2002, the IG recommended that General Hayden formally delegate authority to NSA operational personnel, some of whom had unknowingly violated terms of the Authorization. The Counsel to the Vice President, demanding secrecy, refused to let them see terms of the authority, which had been delegated by the President to the Secretary of Defense, who delegated it to the Director of NSA. General Hayden issued the first "Delegation of Authority" letter to key operational personnel in the SID on 4 March 2003. Subsequent delegation letters were issued each time the President renewed the authority.

(C) Second, in March 2003, the IG advised General Hayden that he should report violations of the Authorization to the President. In February of 2003, the OIG learned of PSP incidents or violations that had not been reported to overseers as required, because none had the clearance to see the report.

(TS//SI//OC/NF) Before March 2003, NSA quarterly reports on intelligence activities sent to the President's Intelligence Oversight Board (through the Assistant to the Secretary of Defense for Intelligence Oversight) stated that the Director was not aware of any unlawful surveillance activities by NSA other than that described in the report. Beginning in March 2003, at the IG's direction, NSA quarterly reports stated that except as disclosed to the President, the Director was not aware of any unlawful surveillance activities by NSA. Also beginning in March 2003, PSP violations, including those not previously reported to the Intelligence Oversight Board, were reported in "Presidential Notifications."

(U//FOUO) Third, shortly after learning about the Program, the IG participated in a September 2002 meeting of key cleared personnel at which important PSP matters were discussed. He recommended that these types of meetings be held every month. As a result, monthly "due diligence" meetings were held until the Program ended.

WORKING DRAFT

This page intentionally left blank.